UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,385	01/06/2004	Hashem M. Ebrahimi	1565.066US1	6809

21186 7590 11/04/2009

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
11/04/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@slwip.com
request@slwip.com

Office Action Summary	Application No.	Applicant(s)	
	10/752,385	EBRAHIMI ET AL.	
	Examiner	Art Unit	
	CANH LE	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6,8,10 and 12-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-2, 6, 8, 10, 12-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/27/2009 has been entered.

This Office Action is in response to the communication filed on 08/27/2009.

Claims 3-5, 7, 9, 11, and 22-30 have been cancelled.

Claims 1, 6, 8, and 16 have been amended.

Claims 1-2, 6, 8, 10, 12-21 have been examined and are pending.

Response to Arguments

Applicant's arguments, see page 7, filed 07/27/2009, with respect to the specification have been fully considered. The objection of the specification has been withdrawn due to amendment.

Applicant's arguments, see page 8, filed 07/27/2009, with respect to claims 1, 10, 14, and 20 have been fully considered. The objection of claims 1, 0, 14, and 20 has been withdrawn due to amendment.

Applicant's arguments filed 07/27/2009 have been fully considered but they are not persuasive.

The Applicant argues the following:

(a) The proposed combination of Subramaniam, Barton and Bazot fails to teach or suggest any notion of detection of a true insecure reference that has been tampered with, such a reference that include a cookie with its metadata or header.

The Examiner respectfully disagrees with the Applicant for the following reasons:

Per (a):

Barton positively discloses a detection of a true insecure reference that has been tampered with *[Barton: par. [0012]; scanning code operable to scan said data at said proxy computer for illegal content (i.e. a true insecure reference); See also par. [0014], [0018]; par. [0033]; if illegal content is found (i.e. a true insecure reference has been tampered), then this trigger an appropriate action such as sending of a warning webpage to a client ...The secure connection would also be terminated; fig. 4, par. [0039]].*

Bazot positively discloses reference that includes a cookie with its metadata or header *[Bazot: abstract; cookie containing information about the user's session (i.e. metadata); par. [0008]; when returning an HTTP object to a client, the server also sends a cookie that the client will store ... Any future HTTP request made by the client which fall in that range will include a transmittal of the current value of the cookie ... the cookie contain sensitive information that could be potentially used for hacking].*

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-2, 6, and 16-21 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended claim (claim 1) recites the limitation "identifies ***a true insecure reference*** by determining that ***the true insecure reference*** is ***a particular reference that has been determined to have been tampered with***" (emphasis added). However, the aforementioned limitation **was not defined** in the specification *(see page 10, lines 29-31; "A potentially insecure reference is a true insecure reference when the processing of the method 200 determines the content or metadata of the reference has been tampered with or is associated with a known insecure reference)*. As a result, the specification fails to convey to one skilled in the art at the time the application was filed, that the inventor(s) had possession of the claimed invention. The Examiner respectfully requests the Applicant **specifically** point out and **explain** where in the specification support can be found for the aforementioned newly added limitations. Applicant is required to cancel the new matter in the reply to this Office Action.

Claims 2 and 6 are dependent on claim 1, and therefore inherit the 35 U.S.C 112, first paragraph as failing to comply with the written description requirement of the independent claims.

The amended claim (claim 16) recites the limitation *"**true insecure references** identified **as particular references having metadata that are associated with World-Wide Web cookies**"* (emphasis added). However, the aforementioned limitation **was not defined** in the specification *(See page 16, lines 20-22; "This may be useful, when the removed references are known to insecure or determine to have been tampered in some way. For example, the metadata or header associated with a removed reference link may include a cookie").* As a result, the specification fails to convey to one skilled in the art at the time the application was filed, that the inventor(s) had possession of the claimed invention. The Examiner respectfully requests the Applicant **specifically** point out and **explain** where in the specification support can be found for the aforementioned newly added limitations. Applicant is required to cancel the new matter in the reply to this Office Action.

Claims 17-21 are dependent on claim 16, and therefore inherit the 35 U.S.C 112, first paragraph as failing to comply with the written description requirement of the independent claims.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 20 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 20 recites the limitation "the denial" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-2, 6, 8, 10, and 12-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject mater.

Regarding to claims 1 and 8, the claims invention are not directed to eligible subject matter under 35 U.S.C § 101 in view of the machine-or-transformation test **(M-or-T test).** In accordance with the M-or-T test, the claimed process must:

(1) be tied to a particular machine; or

(2) particularly transform a particular article to a different state or thing.

The instant claims are neither positively tied to a *particular machine* that accomplishes the claimed method steps nor *particularly transform* underlying subject matter; Therefore, the claimed invention is directed to non-statutory subject matter.

Claims 2 and 6 are rejected under 35 U.S.C. 101 for the same reasons.

Claims 10 and 12-15 are rejected under 35 U.S.C. 101 for the same reasons.

Claim 16 recites in the preamble *"A secure communications management system... comprising: a secure communication manager and a proxy".* Although the preamble of the claim recites "**a system,**" the body of the claim does not positively recite any element of hardware (i.e. "**a secure communication manager**", "**a proxy**"). In view of the publication

specification (pg. 12, line 25 to pg. 14 line 30, fig. 3), said secure communication manager and proxy can be implemented in software. Therefore, the claim is directed to non-statutory subject matter.

Claims 17-21 are rejected under 35 U.S.C. 101 for the same reasons.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 6, 8, 13, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Subramaniam** et al. (US Patent: 6,081,900) in view of **Barton** et al. (US 2003/0131259 A1) further in view of **Bazot** et al. (US 2004/0073629 A1).

As per claim 1:

Subramaniam teaches a method to manage secure communications implemented in a computer-readable medium and to execute on a proxy the method, comprising:

(a) establishing a secure session on a secure site with an external client that communicates from an insecure site **[Subramaniam : Col. 3 lines 35-50; Col. 3, line 66 to Col. 4 line 17]**;

(b) detecting access attempts during the secure session directed to insecure transactions, the insecure transactions identified as links to a site **[Subramaniam : Col. 6, lines 40-60; By checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102. The target server 104 check user permission against access control list associated with the data"; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ...which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19]** *[[(external site) to, not controlled by, and not recognized by the secure site, and wherein the access attempts are directed to the insecure transactions having references to resources of the external site]*; and

(c) transparently managing the access attempts by pre-acquiring content from the external site by accessing the links on behalf of the external client to pre-acquire the content and by scanning and inspecting the content within the secure site before determining whether the content should be made available to the external client during the secure session **[Subramaniam : Col. 6, lines 40-60; The target server 104 check u*ser* permission against access control list associated with the data, or take other steps to make sure the requesting user is entitled to access the request data before providing data"; fig. 1, Border server 106 includes URL**

transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ….which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19; Col. 5; lines 25-27; "The secure network 100 includes one or more file or object or Web servers such as target server 104"; figs. 1, 3; The target server 104 is in the secure network 100; Col. 10, lines 59-66; "The target server 104 can then transform any non-secure data 130 to the border server 106 for subsequent transmission to the external client 112."], *[[and wherein at least one access attempt associated with at least one piece of the content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined to have been tampered with, and wherein the true insecure reference is entirely removed from the content before the content is supplied to the external client.]].*

Subramaniam does not explicit disclose wherein the border server is external from the secure site, wherein at least one access attempt associated with at least one piece of the content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined to have been tampered with, and wherein the true insecure reference is entirely removed from the content before the content is supplied to the external client.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the border server to an site external from the secure location, since it has been held that it requires routine skill in the art to rearrange the location of the border server because it would not have modified the operation of the device **[See MPEP 2144.04; see also *In re Japikse,* 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)].**

Barton discloses transferring data via a secure network connection, wherein at least one access attempt associated with at least one piece of the content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined to have been tampered with **[Barton: par. [0012]; scanning code operable to scan said data at said proxy computer for illegal content (i.e. a true insecure reference); See also par. [0014], [0018]; par. [0033]; if illegal content is found (i.e. a true insecure reference has been tampered), then this trigger an appropriate action such as sending of a warning webpage to a client ...The secure connection would also be terminated; fig. 4, par. [0039]]**, *[[wherein the true insecure reference is entirely removed from the content before the content is supplied to the external client]].*

Therefore, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Barton with the teaching of Subramaniam, wherein at least one access attempt associated with at least one piece of the content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined to have been tampered with to ensure that a transferring data does not contain any illegal content by scanning for illegal content before data is delivered to a client **[Barton: par. [0014]].**

Subramaniam and Barton do not explicitly disclose wherein the true insecure reference is entirely removed from the content before the content is supplied to the external client.

However, Bazot discloses method of accessing Internet resources through a proxy with improved security, wherein the true insecure reference is entirely removed from the content before the content is supplied to the external client **[Bazot: abstract; fig. 2; par. [0008]; when returning an HTTP object o a client, the server also sends a cookie that the client will store. Included in such a cookie is domain information indicating in which domain the cookie is valid. Any future HTTP request made by the client which fall in that range will include a transmittal of the current value of the cookie … the cookie contain sensitive information that could be potentially used for hacking purpose; par. [0010]; transmitting a response to a user after cookie(s) has (have) been removed from the response; See also par. [0019-0020]].**

Therefore, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Bazot with the teaching of Subramaniam and Barton, wherein the true insecure reference is entirely removed from the content before the content is supplied to the external client to provide users with a means for accessing Internet resource through a proxy with improved security by preventing cookies from being downloaded and potentially analyzed by a user or a hacker taking a place of the user **[Bazot: par. [0002], [0009]].**

As per claim 2:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam further teaches the method of claim 1 wherein the detecting further includes translating any non-secure links into secure links for some of the insecure transactions before presenting results of the access attempts to the external client **[Subramaniam: Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)]**.

As per claim 6:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam further teaches the method of claim 1 wherein managing includes at least one or more of:

issuing alerts **[Subramaniam: Col. 11, lines 61-67]**, notifications **[Subramaniam: Col. 8, lines 40-57]**, or advisories to a monitoring entity or log.

As per claim 8:

Subramaniam teaches a method to manage secure communications implemented in a computer-readable medium and to execute on a proxy the method, comprising:

(a) detecting insecure transactions occurring during a secure session, wherein the insecure transactions result from actions requested by an external client participating in the secure session **[Subramaniam: Col. 6, lines 40-60; By checking the IP address which the request was made, the target server 104 determines that the request came from outside the security parameter 102]**;

(b) inspecting the insecure transactions in advance of satisfying the actions requested by pre- acquiring content associated with the insecure transactions before making available to the external client, and wherein the insecure transactions are associated with links to an external site *[[located outside a secure site associated with the secure session]]*, and wherein content are pre-acquired from the external site via the links and inspected and scanned on behalf of the external client within the proxy **[Subramaniam : Col. 6, lines 46-60; A target server check user permissions against access control lists; fig. 1, Border server 106 includes URL transformer 108 and cache(s) 110; fig. 3; Border server 106; Col. 9, lines 32-43; "The possibly repeated acts within the transmitting step 128 involve sending one or more Web pages, files, or other pieces of non-secure data 130 from the target server 104 to the border server 106. The data 130 is non-secure in that it includes hypertext links, URLs, or other references which, if presented by the external client 112 to the secure network 100, ...which contain URLs specifying "http://" rather than "https://" in reference to data stored on the target server 104 are examples of non-secure data 130"; Col. 10, lines 10-19; Col. 5, lines 42-49; proxy servers]**; and

(c) making a determination based on the inspection for taking processing actions including one or more of the following:

permitting some of the insecure transactions to proceed in a modified fashion **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)]** *[[and denying some of the insecure transactions by denying the actions requested, and wherein some of the insecure transactions that are denied are identified as references that have a World-Wide Web (WWW) cookie associated with their*

headers, and wherein these references are entirely removed from the content before the content is supplied to the external client.]].

Subramaniam does not explicitly disclose wherein the border server is external from secure site, denying some of the insecure transactions by denying the actions requested, and wherein some of the insecure transactions that are denied are identified as references that have a World-Wide Web (WWW) cookie associated with their headers, and wherein these references are entirely removed from the content before the content is supplied to the external client.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to move the border server to an site external from the secure location, since it has been held that it requires routine skill in the art to rearrange the location of the border server because it would not have modified the operation of the device **[See MPEP 2144.04; see also *In re Japikse,* 181 F.2d 1019, 86 USPQ 70 (CCPA 1950)].**

Barton discloses transferring data via a secure network connection, wherein denying some of the insecure transactions by denying the actions requested, and wherein some of the insecure transactions that are denied are identified as references **[Barton: par. [0012]; scanning code operable to scan said data at said proxy computer for illegal content; See also par. [0014], [0018]; par. [0033]; if illegal content is found, the this trigger an appropriate action such as sending of a warning webpage to a client ...The secure connection would also be terminated; fig. 4, par. [0039]]** *[[that have a World-Wide Web (WWW) cookie associated with their headers, and wherein these references are entirely removed from the content before the content is supplied to the external client.]].*

Therefore, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Barton with the teaching of Subramaniam to ensure that a transferring data does not contain any illegal content by scanning for illegal content before data is delivered to a client **[Barton: par. [0014]]**.

Subramaniam and Barton do not explicitly disclose wherein World-Wide Web (WWW) cookie associated with their headers, and wherein these references are entirely removed from the content before the content is supplied to the external client.

However, Bazot discloses method of accessing Internet resources through a proxy with improved security, wherein World-Wide Web (WWW) cookie associated with their headers **[Bazot: abstract; cookie containing information about the user's session; par. [0008]; when returning an HTTP object to a client, the server also sends a cookie that the client will store. Included in such a cookie is domain information indicating in which domain the cookie is valid. Any future HTTP request made by the client which fall in that range will include a transmittal of the current value of the cookie]**, and wherein these references are entirely removed from the content before the content is supplied to the external client **[Bazot: abstract; fig. 2; par. [0010]; transmitting a response to a user after cookie(s) has (have) been removed from the response; See also par. [0019-0020]]**.

Therefore, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Bazot with the teaching of Subramaniam and Barton, wherein the true insecure reference is entirely removed from the content before the content is supplied to the external client to provide users with a means for accessing Internet resource through a proxy with improved security by preventing cookies from being downloaded

and potentially analyzed by a user or a hacker taking a place of the user **[Bazot: par. [0002], [0009]].**

As per claim 13:

Subramaniam further discloses the method of claim 8 wherein the making a determination further includes permitting some of the insecure transactions to proceed in a modified fashion by transparently processing the external client access attempt within a proxy making the external client access attempt appear to be part of the secure session **[Subramaniam: Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

As per claim 16:

This claim has limitations that are similar to those of claims 1 and 8, thus it is rejected with the same rationale applied against claims 1 and 8 above.

As per claim 17:

Subramaniam further discloses the secure communications management system of claim 16 wherein the secure communications manager translates Hypertext Transfer Protocol (HTTP) insecure communications into HTTP over Secure Sockets Layer (HTTPS) secure communications during the secure session **[Subramanian : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure e URLs (i.e. HTTPs)].**

Claims 10, 12, 14-15, and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Subramaniam** et al. (US Patent: 6,081,900) in view of **Barton** et al. (US 2003/0131259 A1) further in view of **Bazot** et al. (US 2004/0073629 A1), and further in view of "Netscape Proxy Server Administrator's Guide Version 3.5 for Unix", 1997, as provided by applicant herein after **Netscape_unix_v3.5.**

As per claim 10:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam further discloses a method permitting the insecure transactions to proceed in the modified fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links to HTTP over Secure Sockets Layer (HTTPS) **[Subramaniam : Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)].**

Subramaniam, Barton, and Bazot do not disclose to suppress security warning messages.

However, Netscape_unix_v3.5 discloses to suppress security warning messages **[Netscape_unix_v3.5: Chapter 10, pages 1-3; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be an empty text].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Bazot by including the

teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 12:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam discloses a method permitting insecure transactions to proceed unmodified **[Subramaniam: Col. 2, lines 36-41].**

Subramaniam, Barton, and Bazot do not explicitly disclose permitting normally occurring security warnings to be presented to the client before satisfying the external client access attempt to reference the external site.

However, Netscape_unix_v3.5 discloses permitting normally occurring security warnings to be presented to external the client before satisfying the external client access attempt to reference the external site **[Netscape_unix_v3.5 : Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Bazot by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning

webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 14:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam, Barton, and Bazot do not explicitly disclose method, wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of a denial.

However, Netscape_unix_v3.5 discloses a method wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of a denial **[Netscape_unix_v3.5: Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Bazot by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 15:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam, Barton, and Bazot do not explicitly disclose the method of claim 8 wherein the making a determination further includes denying the some of the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt.

However, Netscape_unix_v3.5 discloses a method wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt **[Netscape_unix_v3.5 : Chapter 13, pages 1-7].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Bazot by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 18:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam further discloses the secure communications management system of claim 16 wherein the proxy selectively modifies a number of the insecure communications **[Subramaniam : Col. 3, lines 34-51; Col. 3, line 66 to Col. 4, line 8].**

Subramaniam, Barton, and Bazot do not explicitly disclose to suppress normally occurring security warning messages that the secure communications manager issues.

However, Netscape_unix_v3.5 discloses to suppress normally occurring security warning messages that the secure communications manager issues **[Netscape_unix_v3.5 : Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Bazot by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 19:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam further discloses the secure communications management system of claim 16 wherein the proxy selectively leaves a number of the insecure communications unchanged **[Subramaniam: Col. 2, lines 36-41].**

Subramaniam, Barton, and Bazot do not explicitly disclose to issue security warning messages to the external client.

However, Netscape_unix_v3.5 discloses a proxy sending security warning messages to the external client **[Netscape_unix_v3.5 : Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Bazot by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 20:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam, Barton, and Bazot do not explicitly disclose a proxy which selectively denies a number of the insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log.

However, Netscape_unix_v3.5 discloses a proxy which selectively denies a number of the insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log **[Netscape_unix_v3.5 : Chapter 13, page 1; A**

proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt; Proxy error log messages include Catastrophe error, Failure, information log entry, warning flags, and security warning].

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Bazot by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

As per claim 21:

The combination of Subramaniam, Barton, and Bazot teach the subject matter as described above.

Subramaniam, Barton, and Bazot do not disclose a proxy selectively sending custom warning messages or explanations to the external client regarding a number of the insecure communications.

However, Netscape_unix_v3.5 discloses a proxy which selectively issues custom warning messages or explanations to the external client regarding a number of the insecure communications **[Netscape_unix_v3.5: Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages].**

Thus, it would have been obvious to one person of ordinary skill in the art at the time the invention was made to combine the method of Subramaniam, Barton, and Bazot by including the teaching of Netscape_unix_v3.5 because it would improve warning techniques for managing secure warning communications by triggering appropriate action such as sending of a warning webpage to client or an issue of an alert message to a network administrator **[Barton: par. [0033]].**

Conclusion

The examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claims. That is, indicate support for newly added claim language by specifically pointing to page(s) and line number(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application. Failure to show support can result in a non-compliant response.

When responding to this office action, Applicant is advised that if Applicant traverses an obviousness rejection under 35 U.S.C. 103, a reasoned statement must be included explaining why the Applicant believes the Office has erred substantively as to the factual findings or the conclusion of obviousness See 37 CFR 1.111(b).

Additionally Applicant is further advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

US 20030208570 A1 to Lapidous, Eugene;

US 20030061387 A1 to Brown, Frances C. et al.;

US 7370351 B1 to Ramachandran; Viyyokaran Raman et al.;

US 6961759 B2 to Brown; Frances C. et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Orgad Edan can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

October 25, 2009

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434